AWS Cloud Infrastructure Improvement of Security Plan

Recommendations of the CloudShield team

Frederico Rosa

Gonçalo Afonso

Tatiana Meneses

Tiago Duarte

Executive Summary

On March 6th, the CloudShield team received an email from Mr. James Reynolds, Chief Security Officer, from the Titan Industrial Solutions company. The client is seeking an enhancement of their cloud security to protect against cyber threats, industrial espionage, and unauthorized access attempts.

The following document provides a clear understanding of how the CloudShield team built a completely secure AWS infrastructure, that provides a safe environment for all users.

Table of Contents

1. Cybersecurity risk analysis

With the evolution of society and technology, cyber attacks have increased exponentially. Information in digital format and all the assets of a network can be considered a threat actor. This is why it is extremely important for an organization to have a detailed, well established, risk management strategy.

According to the National Institute of Standards and Technology (NIST), cybersecurity is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." (https://csrc.nist.gov/glossary/term/cybersecurity).

Titan Industrial Solutions is a company that operates a network of IoT-connected manufacturing facilities and relies on a AWS platform to manage critical infrastructure. This makes it even more important to develop a risk management strategy and policy, in order to protect all of the company's assets.

If the company's AWS infrastructure is not well configured a lot of security risks can happen. For example, if a user has a weak authentication process, the device becomes vulnerable and an easy gateway to execute other attacks (such as DDoS and execution of malware). IoT devices also tend to use the same network as other endpoints. This makes the devices become easy targets for hackers to gain access to sensitive data. Another risk that these devices bring is the high probability of lack of software updates. If the devices are not updated with the latest software, threat actors might gain access without much effort.

For all of these reasons, and more, the CloudShield team developed a well established incident response plan, so that the cybersecurity department can implement safe security measures in order to mitigate a threat.

2. AWS Cloud Infrastructure risk identification

While working with Titan Industrial Solutions infrastructure there were some clear concerns and risks identified:

- operates a network of IoT-connected;
- low level of security management of IoT (weak passwords, outdated softwares);
- insecure data transfer and storage;
- lack of device management;
- lack of services and configurations compliant with legal requirements (such as GDPR);
- low level of cloud security;

It is important to understand that IoT devices are a very high risk security level, due to the weak authentication and authorization practices they hold. Which is why it is important to define a clear strategy to keep track of the devices in the network and infrastructure.

3. Risk assessment and safeguards

Titan Industrial Solutions is a company that collects, store's and uses personal and critical information. For this reason, it is important to determine and outline access limitations and prioritize secure measures to protect all stored data. After you determine which assets are crucial to the company, you should:

- confirm employee access authorization (and limit, if necessary);
- maintain a secure strategy to ensure IoT are updated;
- change passwords;
- create new encryption keys and redo the encryption process, for both data at rest and in transit;

4. Incident detection

After ensuring that all of the assets are protected, we need to reevaluate the detection mechanisms and verify the missing data (if necessary). It is important to:

- confirm what kind of data is missing;
- analyze and redo, if necessary, any scripts that provide automate detection;
- verify the services that provide alerts and alarms (such as GuardDuty and CloudWatch);
- confirm what kind of alerts were received in the past 6 months;
- verify the firewall for misconfigurations;
- verify logs for any unusual network activity (for the past 6 months);
- update any software, anti-virus or anti-malware outdated;
- send a report to the data controller detailing the level of risk and its impact on the company (or country, if the incident might possibly have a national impact);